Sur la théorie de Breuil-Kisin II

Introduction

Fixons d'abord quelques notations :

– soit k un corps parfait de caractéristique $p > 0$, $W = W(k)$ l'anneau des vecteurs de Witt, $K_0 = \mathrm{Fr}(W)$ le corps des fractions de W ;

– K/K_0 une extension totalement ramifiée de degré e de K_0 et $\pi \in K$ une uniformisante fixée avec $E(u) \in W[u]$ son polynôme minimal.

– Notons $\mathbf{BT}(\mathcal{O}_K)$ la catégorie des groupes p-divisibles sur $\mathcal{O}_K$ (à isomorphisme près).

– Notons S le complété p-adique de

$$W[u]\left[\frac{E(u)^i}{i!} : i = 1, 2 \ldots\right] \subset K_0[u],$$

et $\mathrm{Fil}^1 S \subset S$ la fermeture de l'idéal engendré par $E(u)^i/i!$ $(i = 1, 2, \ldots)$.

* S est muni d'un endomorphisme de Frobenius φ tel que $\varphi(u) = u^p$ et que φ agisse sur $W \subset S$ via le Frobenius de W ;

* $\varphi(\mathrm{Fil}^1 S) \subset pS$. Ainsi, le morphisme $\varphi_1 := \varphi/p \colon \mathrm{Fil}^1 S \to S$ est bien défini.

* Il y a un morphisme naturel

$$W[u]\left[\frac{E(u)^i}{i!} : i = 1, 2 \ldots\right] \longrightarrow \mathcal{O}_K, \quad u \mapsto \pi,$$

induisant $S/\mathrm{Fil}^1 S \xrightarrow{\sim} \mathcal{O}_K$.

Définition 0.1. *Notons $\mathbf{BT}^{\varphi}_{/S}$ la catégorie des S-modules, où un objet est la donnée*

– *d'un S-module $\mathscr{M}$ libre de rang fini ;*

– *d'un sous-S-module $\mathrm{Fil}^1\mathscr{M} \subset \mathscr{M}$ tel que $\mathrm{Fil}^1 S \cdot \mathscr{M} \subset \mathrm{Fil}^1\mathscr{M}$ et que le quotient $\mathscr{M}/\mathrm{Fil}^1\mathscr{M}$ soit un $\mathcal{O}_K$-module sans p-torsion (donc libre de rang fini sur $\mathcal{O}_K$) ;*

– *d'un morphisme φ-semi-linéaire $\varphi_{1,\mathscr{M}} \colon \mathrm{Fil}^1\mathscr{M} \to \mathscr{M}$ tel que $\mathscr{M}$ soit engendré en tant que S-module par $\varphi_{1,\mathscr{M}}(\mathrm{Fil}^1\mathscr{M})$.*

Théorème 0.2 (Breuil pour $p > 2$,Kisin pour $p = 2$)**.** *Il existe un foncteur exact contravariant*

$$\underline{\mathscr{M}} \colon \mathbf{BT}^{\varphi}_{/S} \to \mathbf{BT}(\mathcal{O}_K),$$

qui est une équivalence pour $p > 2$. Si $p = 2$, ce dernier foncteur induit une équivalence sur les catégories à isogénie près.

Le but de cet exposé est de donner la preuve de Kisin de Théorème 0.2 (pour $p > 2$), et de présenter un résultat auxiliaire (Proposition 3.1) qu'on a besoin pour démontrer le theorem de Kisin (également le cas $p > 2$).

1 Construction de $\underline{\mathscr{M}}$.

1.1 Rappel d'un lemme technique

Soient A_0 une $\mathbb{Z}_p$-algèbre locale séparée et complète pour la topologie p-adique de corps résiduel k, et $G \in \mathbf{BT}(A_0)$. Alors le noyau $p^n A \subset A$ du morphisme surjectif $A_0 \to A_0/p^n A_0$ est muni d'une structure à PD. Ainsi, ceci nous permet de considérer

$$\mathbb{D}(G)(A_0) := \varprojlim_i \left(\mathbb{D}(G \otimes_{A_0} A_0/pA_0)_{\mathrm{Spec}(A_0/pA_0) \hookrightarrow \mathrm{Spec}(A_0/p^i A_0)}\right),$$

qui s'insère dans la suite exacte courte suivante

$$0 \longrightarrow \omega_G \longrightarrow \mathbb{D}(G)(A_0) \longrightarrow \mathcal{L}ie(G^D) \longrightarrow 0.$$ [1]

Soit en outre $A \to A_0$ est un morphisme surjectif de $\mathbb{Z}_p$-algèbres séparés et complètes pour la topologie p-adique dont le noyau $\mathrm{Fil}^1 A$ est muni de puissances divisées **compatibles aux PD sur** $pA \subset A$. Alors pour chaque i, le noyau du morphisme $A/p^i A \to A_0/pA_0$ est encore muni de PD. D'où

$$\mathbb{D}(G)(A) := \varprojlim_i \left(\mathbb{D}(G \otimes_{A_0} A_0/pA_0)_{\mathrm{Spec}(A_0/pA_0) \hookrightarrow \mathrm{Spec}(A/p^i A)}\right).$$

Si de plus A admet un endomorphisme φ qui est un relèvement du Frobenius de A/pA, on dispose alors d'un morphisme φ-semilinéaire de A-modules, toujours noté par φ :

$$\varphi \colon \mathbb{D}(G)(A) \to \mathbb{D}(G)(A).$$

On rappelle le lemme suivant, que nous l'avons vu dans l'exposé de Dajano.

Lemma 1.1. *Soit $f \colon A \to A_0$ un morphisme surjectif de $\mathbb{Z}_p$-algèbres séparés et complètes pour la topologie p-adique.* [2] *et que le noyau $\mathrm{Fil}^1 A$ de f est muni de puissances divisées. Supposons en outre les deux conditions suivantes :*

1. *A est sans p-torsion, et est muni d'un endomorphisme $\varphi \colon A \to A$ relevant le Frobenius sur A/pA ;*
2. *L'application $\varphi^*(\mathrm{Fil}^1(A)) \xrightarrow{1 \otimes \varphi/p} A$ est surjective.*

Soit G un groupe p-divisible sur A_0, et posons $\mathrm{Fil}^1(\mathbb{D}(G)(A))$ l'image réciproque de $\omega_G \subset \mathbb{D}(G)(A_0)$. Alors la restriction du morphisme $\varphi \colon \mathbb{D}(G)(A) \to \mathbb{D}(G)(A)$ à $\mathrm{Fil}^1(\mathbb{D}(G)(A))$ est divisible par p, et le morphisme induit

$$1 \otimes \varphi/p \colon A \otimes_{\varphi, A} \mathrm{Fil}^1 \mathbb{D}(G)(A) \longrightarrow \mathbb{D}(G)(A)$$

est surjectif.

1. In faut faire attention qu'ici, $\omega_G := \varprojlim \omega_{G \otimes_{A_0} A_0/p^n A_0}$, et même pour $\mathcal{L}ie(G^D)$.
2. À noter que $p \in A_0$ n'est pas supposé nilpotent.

1.2 Application

Considérons le morphisme $S \to \mathcal{O}_K$ $(u \mapsto \pi)$, dont le noyau est donné par $\mathrm{Fil}^1 S \subset S$. Soit $G \in \mathbf{BT}(\mathcal{O}_K)$. La construction et le lemme dans du numéro précédent (appliqués au cas où $A_0 = \mathcal{O}_K$ et $A = S$) nous fournissent un foncteur

$$\underline{\mathscr{M}}\colon \mathbf{BT}(\mathcal{O}_K) \longrightarrow \mathbf{BT}^{\varphi}_{/S}, \quad G \mapsto (\mathbb{D}(G)(S), \mathrm{Fil}^1\mathbb{D}(G)(S), \varphi/p).$$

En effet, comme $\mathrm{Fil}^1\mathbb{D}(G)(S)$ la préimage de $\mathrm{Fil}^1\mathbb{D}(G)(\mathcal{O}_K) \subset \mathbb{D}(G)(\mathcal{O}_K)$ par la surjection canonique $\mathbb{D}(G)(S) \to \mathbb{D}(G)(\mathcal{O}_K)$. Donc $\mathrm{Fil}^1\mathbb{D}(G)(S) \supset \mathrm{Fil}^1 S \cdot \mathbb{D}(G)(S)$, et

$$\mathbb{D}(G)(S)/\mathrm{Fil}^1\mathbb{D}(G)(S) \xrightarrow{\sim} \mathbb{D}(G)(\mathcal{O}_K)/\omega_G \xrightarrow{\sim} \mathcal{L}ie(G^D)$$

qui est sans p-torsion. Les autres conditions de $\mathbf{BT}^{\varphi}_{/S}$ sont aussi faciles à vérifier à l'aide de Lemme 1.1.

Exemple 1.2. A titre d'exemple, on a $\underline{\mathscr{M}}(\mathbb{Q}_p/\mathbb{Z}_p) = (S, \mathrm{Fil}^1 S, \varphi/p)$, et $\underline{\mathscr{M}}(\mu_{p^\infty}) = (S, S, \varphi)$.

Ainsi, pour démontrer Theorem 0.2, on doit construire un quasi-inverse $\underline{\mathscr{G}}$ (à isogénie près si $p = 2$)

2 Preuve de Théorème 0.2 (cas $p > 2$)

2.1 Encore un lemme technique

Dans ce qui suit, un **anneau spécial** est une $\mathbb{Z}_p$-algèbre locale de corps résiduel k, séparée et complète pour la topologie p-adique, sans p-torsion et mui d'un endomorphisme φ qui relève le Frobenius de A/pA. Pour un tel anneau A, on désigne par $\mathcal{C}_A$ la catégorie des triples $(\mathscr{M}, \mathscr{M}_1, \varphi_{\mathscr{M}})$, où

- $\mathscr{M}$ est un A-module libre de rang fini ;
- $\varphi_{\mathscr{M}}\colon \mathscr{M} \to \mathscr{M}$ est un morphisme φ-semi-linéaire ; et
- $\mathscr{M}_1 \subset \mathscr{M}$ est un sous-A-module tel que $\varphi_1(\mathscr{M}_1) \subset p\mathscr{M}$ et que $A\cdot(\varphi_{\mathscr{M}}/p)(\mathscr{M}_1) = \mathscr{M}$.

Soit $A \to B$ un morphisme d'anneaux spéciaux (*i.e.*, un morphisme de $\mathbb{Z}_p$-algèbre compatible aux Frobenius), on a un foncteur canonique

$$\mathcal{C}_A \longrightarrow \mathcal{C}_B, \quad (\mathscr{M}, \mathscr{M}_1, \varphi_{\mathscr{M}}) \mapsto (\mathscr{M} \otimes_A B, \mathrm{Im}(\mathscr{M}_1 \otimes_A B \to \mathscr{M} \otimes_A B), \varphi_{\mathscr{M}} \otimes 1).$$

Lemma 2.1. *Soit $h\colon A \to B$ un morphisme surjectif d'anneau spéciaux de noyau $J \subset A$. Supposons $\varphi^i(J) \subset p^{i+j_i}J$ $(i \geq 1)$ avec $\{j_i\}_i$ une suite d'entiers vérifiant $\varinjlim_i j_i = +\infty$ et $j_1 \geq 0$. Soient $\mathscr{M}, \mathscr{M}'$ deux objets de $\mathcal{C}_A$, et $\theta_B\colon \mathscr{M} \otimes_A B \xrightarrow{\sim} \mathscr{M}' \otimes_A B$ un isomorphisme dans $\mathcal{C}_B$. Il existe alors un unique isomorphisme de A-modules $\theta_A\colon \mathscr{M} \xrightarrow{\sim} \mathscr{M}'$ compatible aux Frobenius.*

Démonstration. Soit $\theta_0\colon \mathscr{M} \to \mathscr{M}'$ un morphisme de A-modules qui relève θ_B (c'est possible car $A \to B$ est surjectif). On va construire θ_A à partir de θ_0 par approximation successive. Comme θ_0 relève θ_B qui est un isomorphisme dans $\mathcal{C}_B$, $\theta_0(\mathscr{M}_1) \subset \mathscr{M}'_1 + J\mathscr{M}'$.

Or $\varphi(J) \subset pA$ (car $j_1 \geq 0$), quitte à remplacer $\mathscr{M}_1'$ par $\mathscr{M}_1' + J\mathscr{M}'$, on peut supposer $J\mathscr{M}' \subset \mathscr{M}_1'$. Ainsi $\theta_0(\mathscr{M}_1) \subset \mathscr{M}_1'$.

Montrons d'abord que le morphisme canonique $1 \otimes \varphi_{\mathscr{M}} \colon \varphi^*\mathscr{M} \to \mathscr{M}$ est injectif. En effet, par définition, le morphisme $1 \otimes \varphi_{\mathscr{M}}/p \colon \varphi^*\mathscr{M}_1 \to \mathscr{M}$ est surjectif. Par suite, il est en de même de $(1 \otimes \varphi_{\mathscr{M}})[p^{-1}] \colon \varphi^*\mathscr{M}[1/p] \to \mathscr{M}[1/p]$. Or ce dernier est un morphisme surjectif entre deux $A[1/p]$-modules libres de même rang, il est nécessairement un isomorphisme. Enfin, comme A est sans p-torsion, $\varphi^*\mathscr{M}$ l'est aussi. Par suite, le morphisme canonique $\varphi^*\mathscr{M} \to \varphi^*\mathscr{M}[1/p]$ est injectif. D'où l'injectivité du morphisme $1 \otimes \varphi_{\mathscr{M}}$.

Considérons le morphisme composé, noté par ι

$$\varphi^*(\mathscr{M}_1) \xrightarrow{\varphi^*(\theta_0|_{\mathscr{M}_1})} \varphi^*(\mathscr{M}_1') \xrightarrow{1 \otimes \varphi_{\mathscr{M}'}/p} \mathscr{M}'.$$

Montrons que ι se factorise à travers le morphisme surjectif $1 \otimes \varphi_{\mathscr{M}}/p \colon \varphi^*\mathscr{M}_1 \to \mathscr{M}$. Soit x un élément du noyau de $1 \otimes \varphi_{\mathscr{M}}/p$. Comme $p(1 \otimes \varphi_{\mathscr{M}}/p)$ se décompose comme

$$\varphi^*\mathscr{M}_1 \xrightarrow{\mathrm{can}} \varphi^*\mathscr{M} \xrightarrow{1 \otimes \varphi_{\mathscr{M}}} \mathscr{M},$$

l'image de x par le morphisme canonique $\varphi^*\mathscr{M}_1 \to \varphi^*\mathscr{M}$ est contenue dans le noyau du morphisme injectif $1 \otimes \varphi_{\mathscr{M}} \colon \varphi^*\mathscr{M} \to \mathscr{M}$, donc est 0. Par suite, en vertu du carré commutatif suivant

$$\begin{tikzcd} x \arrow[dd, mapsto] & \varphi^*\mathscr{M}_1 \arrow[r, "\varphi^*(\theta_0|_{\mathscr{M}_1})"] \arrow[dd, "\mathrm{can}"'] & \varphi^*\mathscr{M}_1' \arrow[dd, "\mathrm{can}"] \\ & & \\ 0 & \varphi^*\mathscr{M} \arrow[r, "\varphi^*\theta_0"] & \varphi^*\mathscr{M}' \end{tikzcd}$$

Par suite, $(p\iota)(x) = ((1 \otimes \varphi_{\mathscr{M}'}) \circ \mathrm{can} \circ \varphi^*(\theta_0|_{\mathscr{M}_1}))\,(x) = 0$. Or $\mathscr{M}'$ est sans p-torsion, on trouve $\iota(x) = 0$. Ainsi, il existe un morphisme de A-modules $\theta_1 \colon \mathscr{M} \to \mathscr{M}'$ tel que $\theta_1 \circ (1 \otimes \varphi_{\mathscr{M}}/p) = (1 \otimes \varphi_{\mathscr{M}'}/p) \circ \varphi^*(\theta_0|_{\mathscr{M}_1})$, ou en termes équivalents, $\theta_1 \circ \varphi_{\mathscr{M}}/p = \varphi_{\mathscr{M}'}/p \circ \theta_0 \colon \mathscr{M}_1 \to \mathscr{M}'$. De plus, en modulo J cette dernière égalité, on trouve que θ_1 est encore un relèvement de θ_B. En répétant cette construction, on obtient une suite de morphisme $\{\theta_i\}_{i\geq 1}$ telle que $\theta_i \circ \varphi_{\mathscr{M}}/p = \varphi_{\mathscr{M}'}/p \circ \theta_{i-1}$. Par suite,

$$(\theta_{i+1} - \theta_i) \circ \varphi_{\mathscr{M}}/p = \varphi_{\mathscr{M}'}/p \circ (\theta_i - \theta_{i-1}) \colon \mathscr{M}_1 \longrightarrow \mathscr{M}'.$$

Comme $(\theta_1 - \theta_0)(\mathscr{M}) \subset J\mathscr{M}'$, on a

$$(\theta_{i+1} - \theta_i)((\varphi_{\mathscr{M}}/p)(\mathscr{M}_1)) = (\varphi_{\mathscr{M}'}/p)^i(\theta_1 - \theta_0)(\mathscr{M}_1) \subset (\varphi_{\mathscr{M}'}/p)^i(J\mathscr{M}') \subset p^{j_i}\mathscr{M}'.$$

Or $\varphi_{\mathscr{M}}/p(\mathscr{M}_1)$ engendre $\mathscr{M}$, on trouve $(\theta_{i+1} - \theta_i)(\mathscr{M}) \subset p^{j_i}\mathscr{M}'$. Ainsi, la suite $\{\theta_i\}_i$ converge en un morphisme de A-modules $\theta_A \colon \mathscr{M} \to \mathscr{M}'$ compatible aux Frobenius qui relève également θ_B.

Il nous reste à vérifier l'unicité. Soit θ_A' un autre relèvement de θ_A compatible aux Frobenius. Alors $(\varphi_A - \varphi_A')(\mathscr{M}) \subset p^{j_i}\mathscr{M}'$. Par sutie, $\theta_A = \theta_A'$. La preuve est donc terminée. $\square$

Remarque 2.2. *On va appliquer Lemma 2.1 dans la situation suivante : supposons que l'idéal A est muni de puissances divisées, et qu'il existe un nombre fini d'éléments $x_1, \ldots, x_n \in J$ tel que J soit topologiquement (pour la topologie p-adique) engendré par par x_i et leurs puissances divisées. Supposons en outre que $\varphi(x_i) = x_i^p$. On peut alors prendre $j_i = v_p((p^i - 1)!) - i$.*

2.2 Démonstration de Théorème 0.2 pour $p > 2$

Pour simplifier, on se place ici dans le cas où $p > 2$. On va construire un quasi-inverse de $\underline{\mathscr{M}}$, qui sera noté par $\underline{\mathscr{G}}$.

Soit $(\mathscr{M}, \mathrm{Fil}^1\mathscr{M}, \varphi_{1,\mathscr{M}})$ un objet de $\mathbf{BT}^{\varphi}_{/S}$. Le S-module $\mathscr{M}$ est muni d'un morphisme φ-semi-linéaire :

$$\varphi_{\mathscr{M}} \colon \mathscr{M} \to \mathscr{M}, \quad x \mapsto \varphi_1(E(u))^{-1}\varphi_{1,\mathscr{M}}(E(u)x).$$

Ici, on remarque que $\varphi_1(E(u)) := \varphi(E(u))/p \in S$ est *inversible.*

2.2.1 Construction de $\underline{\mathscr{G}}$ modulo p

Pour $i \geq 1$, posons $R_i = W[u]/u^i$. On munit R_i le Frobenius défini par $\varphi(u) = u^p$. On regarde $\mathcal{O}_K/\pi^i$ comme une algèbre sur R_i via le morphisme de W-algèbres

$$f_i \colon R_i \longrightarrow \mathcal{O}_K/\pi^i\mathcal{O}_K, \quad u \mapsto \pi.$$

Si $i \in \{1, \ldots, e\}$, $\ker(f_i) = pR_i$, par suite f_i définit un épaississement à puissances divisées. D'ailleurs, on dispose d'un morphisme naturel $S \to R_i$ ($u \mapsto u$ et $(u^e)^{[j]} \mapsto 0$ pour $j > 0$). Notons $\mathscr{M}_i = \mathscr{M} \otimes_S R_i$. Avec la définition évidente, on obtient un objet $\mathscr{M}_i \in \mathcal{C}_{R_i}$. On va construire d'abord un groupe p-divisible G_i sur R_i.

Cas où $i = 1$. On a $R_1 = W$ et $\mathcal{O}_K/\pi = k$. Le $W = R_1$-module $\mathscr{M}_1$ est un module de Dieudonné. En effet, il suffit de définir le Verschiebung $V \colon \mathscr{M}_1 \to \mathscr{M}_1$. Comme $1 \otimes \varphi_{1,\mathscr{M}} \colon \varphi^*\mathrm{Fil}^1\mathscr{M}_1 \to \mathscr{M}_1$ est surjectif, il est nécessairement un isomorphism comme le rang de $\mathrm{Fil}^1\mathscr{M}_1$ est inférieur ou égal à celui de $\mathscr{M}_1$. Posons $V = (1 \otimes \varphi_{1,\mathscr{M}_1})^{-1} \colon \mathscr{M}_1 \to \varphi^*\mathrm{Fil}^1\mathscr{M}_1 \subset \varphi^*\mathscr{M}$. Clairement on a $FV = VF = p$, et cela fait $\mathscr{M}_1$ un module de Dieudonné, qui correspond fonctoriellement un objet $G_1 \in \mathbf{BT}(k)$. De plus, on dispose d'un isomorphisme fonctoriel $\mathbb{D}(G_1)(W) \xrightarrow{\sim} \mathscr{M}_1$, et via cet isomorphisme, $\mathrm{Fil}^1\mathbb{D}(G_1)(W)$ (qui est par définition la préimage de $\omega_{G_1} \subset \mathbb{D}(G_1)(\mathcal{O}_K/\pi\mathcal{O}_K)$) s'identifie à $\mathrm{Fil}^1\mathscr{M}_1$ (cf. Lemme 2.3).

Cas où $i \in \{2, \ldots, e\}$. Soit i un tel entier tel qu'on a construit G_{i-1} sur $\mathcal{O}_K/\pi^{i-1}$ avec un isomorphisme $\mathbb{D}(G_{i-1})(R_{i-1}) \xrightarrow{\sim} \mathscr{M}_{i-1}$ compatible aux Frobenius et aux filtrations. Notons que le noyau du morphisme $R_i \to \mathcal{O}_K/\pi^{i-1}$ est (u^{i-1}, p), donc est muni de puissances divisées : $(u^{i-1})^{[j]} = 0$ pour tout $j \geq 2$. On peut donc évaluer $\mathbb{D}(G_{i-1})$ en $R_i \to \mathcal{O}_K/\pi^{i-1}$. On obtient donc deux R_i-modules $\mathbb{D}(G_{i-1})(R_i)$ et $\mathscr{M}_i$. Posons $\mathrm{Fil}^1\mathbb{D}(G_{i-1})(R_i)$ la préimage de $\mathrm{Fil}^1\mathbb{D}(G_{i-1})(R_{i-1})$, ceci fait $\mathbb{D}(G_{i-1})(R_i)$ également un objet de $\mathcal{C}_{R_i}$. D'autre part, par hypothèse de récurrence, on dispose d'un isomorphisme dans $\mathcal{C}_{R_{i-1}}$ entre $\mathbb{D}(G_{i-1})(R_{i-1}) = \mathbb{D}(G_{i-1})(R_i) \otimes_{R_i} R_{i-1}$ et $\mathscr{M}_{i-1} = \mathscr{M}_i \otimes_{R_i} R_{i-1}$. Par Lemma 2.1, ce dernier se relève en l'unique isomorphisme de R_i-modules $\theta_i \colon \mathbb{D}(G_{i-1})(R_i) \to \mathscr{M}_i$ compatible aux Frobenius. Comme le noyau du morphisme $\mathcal{O}_K/\pi^i \to \mathcal{O}_K/\pi^{i-1}$ est à puissances divisées nilpotentes, par Grothendieck-Messing, il existe un relèvement $G_i \in \mathbf{BT}(\mathcal{O}_K/\pi^i)$ de G_{i-1}, fonctoriel en G_{i-1}, tel que $\omega_{G_i} \subset \mathbb{D}(G_{i-1})(\mathcal{O}_K/\pi^i)$ soit égal à l'image du composé

$$\mathrm{Fil}^1(\mathscr{M}_i) \subset \mathscr{M}_i \xrightarrow{\theta_i^{-1}} \mathbb{D}(G_{i-1})(R_i) \xrightarrow{\mathrm{can}} \mathbb{D}(G_{i-1})(\mathcal{O}_K/\pi^i),$$

où le dernier morphisme est induit du morphisme $R_i \to \mathcal{O}_{K/\pi^i}$ (compatible aux puissances divisées sur $(p, u^{i-1}) \subset R_i$ et sur $(u^{i-1}) \subset \mathcal{O}_K/\pi^i$). Ainsi, si l'on munit $\mathbb{D}(G_i)(R_i)$ de la filtration $Fil^1\mathbb{D}(G_i)(R_i)$ donnée par la préimage de $\omega_{G_i} \subset \mathbb{D}(G_i)(\mathcal{O}_K/\pi^i\mathcal{O}_K)$, l'isomorphisme composé $\mathbb{D}(G_i)(R_i) \cong \mathbb{D}(G_{i-1})(R_{i-1}) \xrightarrow{\theta_i} \mathscr{M}_i$ est compatible aux filtrations (voir Lemme 2.3) et aux Frobenius : c'est un isomorphisme dans $\mathcal{C}_{R_i}$.

Lemma 2.3. *Pour $i = 1, \ldots, e$, on a $\mathrm{Fil}^1\mathscr{M}_i = \iota^{-1}(\iota(\mathrm{Fil}^1\mathscr{M}_i))$, où ι est le morphisme surjectif $\iota\colon \mathscr{M}_i \to \mathscr{M}_i \otimes_{R_i} \mathcal{O}_K/\pi^i$.*

Démonstration. Par [1] Lemme 2.1.1.9, il existe une base $(e_1, \ldots, e_d)$ de $\mathscr{M}$ sur S et un entier $d_1 \in \{1, 2, \ldots, d\}$ tels que

$$\mathrm{Fil}^1\mathscr{M} = \left(\oplus_{i=1}^{d_1}\mathrm{Fil}^1 S \cdot e_i\right) \oplus \left(\oplus_{i=d_1+1}^{d} S \cdot e_i\right).$$

Comme l'énoncé de notre lemme ici n'a rien à voir le Frobenius, il suffit de prouver le lemme pour deux cas particuliers : soit $(\mathscr{M}, \mathrm{Fil}^1\mathscr{M}) = (S, S)$, soit $(\mathscr{M}, \mathrm{Fil}^1\mathscr{M}) = (S, \mathrm{Fil}^1 S)$. Le premier cas étant clair car $\mathrm{Fil}^1\mathscr{M} = \mathscr{M}$. On suppose donc $(\mathscr{M}, \mathrm{Fil}^1\mathscr{M}) = (S, \mathrm{Fil}^1 S)$. Par suite, on a

$$\mathrm{Fil}^i\mathscr{M}_i := \mathrm{Im}(\mathrm{Fil}^1\mathscr{M} \otimes_S R_i \longrightarrow \mathscr{M} \otimes_R R_i = \mathscr{M}_i) = h_i(\mathrm{Fil}^1 S)\mathscr{M}_i,$$

où $h_i\colon S \to R_i$ ($u \mapsto u, (u^e)^{[j]} \mapsto 0$ pour $j \geq 1$) est le morphisme canonique. Or comme $i \leq e$, $h_i(E(u)) = p \cdot u_i$ avec $u_i \in R_i^\times$ une unité. Par suite, $j! \cdot h_i(E(u)^{[j]}) = p^j \cdot u_i^j$. D'où $h_i(E(u)^{[j]}) = \frac{p^j}{j!}u_i^j \in pR_i$. Ainsi, on trouve $h_i(\mathrm{Fil}^1 S) = pR_i$, et $\mathrm{Fil}^1\mathscr{M}_i = p\mathscr{M}_i$. D'autre part, $\iota(\mathrm{Fil}^1\mathscr{M}_i) = 0$ (car $i \leq e$), par suite, $\iota^{-1}(\iota(\mathrm{Fil}^1\mathscr{M}_i)) = pR_i$ (car pR_i est le noyau du morphisme canonique $f_i\colon R_i \to \mathcal{O}_K/\pi^i$). Ceci achève la preuve. □

Pour résumé, on a construit un groupe p-divisible $G_e \in \mathbf{BT}(\mathcal{O}_K/\pi^e) = \mathbf{BT}(\mathcal{O}_K/p\mathcal{O}_K)$ et un isomorphisme $\mathbb{D}(G_e)(R_e) \xrightarrow{\sim} \mathscr{M}_e$ compatible aux Frobenius et aux filtrations.

2.2.2 Passage de $\mathcal{O}_K/p\mathcal{O}_K$ à $\mathcal{O}_K$ pour $p > 2$

Le noyau du morphisme $S \to \mathcal{O}_K/p\mathcal{O}_K$ est $\mathrm{Fil}^1 S + pS$, donc est muni de puissances divisées. On peut ansi évaluer le cristal $\mathbb{D}(G_e)$ en cet épaississement : cela nous donne un S-module libre de rang fini $\mathbb{D}(G_e)(S)$ muni d'un morphisme de Frobenius. Posons $\mathrm{Fil}^1\mathbb{D}(G_e)(S)$ la préimage de $\mathrm{Fil}^1\mathbb{D}(G_e)(\mathcal{O}_K/p\mathcal{O}_K) \subset \mathbb{D}(G_e)(\mathcal{O}_K/p)$, cela nous donne alors un objet de $\mathcal{C}_S$ (Lemme 1.1). Par la construction du foncteur $\underline{\mathscr{G}}$ modulo p, on a un isomorphisme dans C_{R_e} : $\mathbb{D}(G_e)(R_e) \xrightarrow{\sim} \mathscr{M}_e$. Par Lemme 2.1, on déduit un unique isomorphisme de S-modules

$$\theta\colon \mathbb{D}(G_e)(S) \xrightarrow{\sim} \mathscr{M}$$

compatible aux Frobenius. Pour relever G_e à $\mathcal{O}_K/p^i\mathcal{O}_K$ ($i \geq 2$), on considère le morphisme $\mathcal{O}_K/\pi^i\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$, dont le noyau est muni de puissances divisées qui sont d'ailleurs *nilpotentes* si $p > 2$. **A partir de maintenant, supposons** $p > 2$.

Comme les puissances divisées du noyau de $\mathcal{O}_K/p^i\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ sont nilpotentes, par Grothendieck-Messing, il existe un unique groupe p-divisible $G_{ie} \in \mathbf{BT}(\mathcal{O}_K/p^i\mathcal{O}_K)$, fonctoriel en G_e, tel que

- G_{ie} est un relèvement de G_e ;
- Le sous-module $\omega_{G_{ie}} \subset \mathbb{D}(G_e)(\mathcal{O}_K/p^i\mathcal{O}_K)$ est égal à l'image du morphisme composé

$$\mathrm{Fil}^1(\mathscr{M}) \subset \mathscr{M} \xrightarrow{\theta^{-1}} \mathbb{D}(G_e)(S) \xrightarrow{\mathrm{can}} \mathbb{D}(G_e)(\mathcal{O}_K/p^i\mathcal{O}_K).$$

Les G_{ie} sont compatibles : $G_{ie}\otimes_{\mathcal{O}_K/p^i\mathcal{O}_K}\mathcal{O}_K/p^{i-1}\mathcal{O}_K \cong G_{(i-1)e}$. La limite projective $\varprojlim_i G_{ie}$ définit donc un objet de $\mathbf{BT}(\mathcal{O}_K)$, noté par $\mathbf{G}(\mathscr{M})$. Par construction, on a $\underline{\mathscr{M}} \circ \underline{\mathscr{G}} \cong \mathrm{id}$. Par ailleurs, par l'unicité de la construction à chaque étape, on a $\underline{\mathscr{G}}(\underline{\mathscr{M}}(G)) \cong G$ modulo p^i pour tout i, par suite, $\underline{\mathscr{G}} \circ \underline{\mathscr{M}} \cong \mathrm{id}$. Ceci finit la preuve de Théorème 0.2 si $p > 2$.

Remarque 2.4. La difficulté pour le cas $p = 2$ provient du fait que les PD sur l'idéal $pS \subset S$ ne sont pas topologiquement nilpotentes. On renvoie à [4] (ou [2]) pour les détails dans le cas $p = 2$.

3 Une relation entre $\mathbf{BT}^{\varphi}_{/\mathfrak{S}}$ et $\mathbf{BT}^{\varphi}_{/S}$

Dans cette section, on démontre un résultat auxiliaire qu'on a besoin pour la preuve de Kisin, énoncé dans l'exposé de Dajano.

On reprise les notations utilisées dans l'exposé de Dajano. En particulier, on a un anneau $\mathfrak{S}$, et un morphisme

$$\mathfrak{S} \to S, \quad u \mapsto u.$$

Considérons le morphisme de W-algèbres ci-dessous, noté par φ dans la suite :

$$\mathfrak{S} \to S, \quad u \mapsto u^p.$$

Pour $(\mathfrak{M}, \varphi_{\mathfrak{M}})$ un objet de $\mathbf{BT}^{\varphi}_{/\mathfrak{S}}$, posons $\mathscr{M} := S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$, qui est naturellement un objet de $\mathbf{BT}^{\varphi}_{/S}$:

- On remarque d'abord que le morphisme canonique $\mathrm{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M} \to S \otimes_{\mathfrak{S}} \mathfrak{M}$ est injectif, et que $\varphi_{\mathfrak{M}}$ induit un morphisme de S-modules

$$1 \otimes \varphi_{\mathfrak{M}} \colon \mathscr{M} = S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \to S \otimes_{\mathfrak{S}} \mathfrak{M}.$$

  Posons $\mathrm{Fil}^1\mathscr{M} \subset \mathscr{M}$ comme la préimage via $1 \otimes \varphi_{\mathfrak{M}}$ de $\mathrm{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M}$.
- $\varphi_{1,\mathscr{M}}$ est le morphisme composé

$$\mathrm{Fil}^1\mathscr{M} \xrightarrow{\text{incl.}} S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \xrightarrow{1\otimes\varphi_{\mathfrak{M}}} \mathrm{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M} \xrightarrow{\varphi_1\otimes 1} S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} = \mathscr{M}.$$ [3]

On obtient donc un foncteur

$$\mathbf{BT}^{\varphi}_{/\mathfrak{S}} \longrightarrow \mathbf{BT}^{\varphi}_{/S}, \quad \mathfrak{M} \mapsto S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}.$$

On a besoin aussi les notations suivantes, introduites déjà dans les exposés précédents :
- $R := \varprojlim_i \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$, et $\mathrm{Fr}(R)$ le corps des fractions de R : c'est un corps algébriquement clos de caractéristique p.
- Soit $\underline{\pi} := (\pi_n)$ une suite d'éléments de $\mathcal{O}_{\overline{K}}$ vérifiant

$$\pi_0 = \pi, \quad \pi_{i+1}^p = \pi_i, \quad i = 0, 1, \dots.$$

  Le morphisme de W-algèbres $W[u] \to W(R)$ ($u \mapsto [\underline{\pi}]$) s'étends en un morphisme injectif de W-algèbres $\mathfrak{S} = W[[u]] \hookrightarrow W(R)$. [4]

3. A noter que $\varphi_1(sx) = \varphi(s)\varphi_1(x)$ pour $s \in S$ et $x \in \mathrm{Fil}^1 S$.
4. à détailler

– Notons $\mathcal{O}_{\mathcal{E}}$ le complété p-adique de $W[[u]][1/u]$, qui est un anneau de valuation discrète de corps résiduel $k((u))$. L'inclusion $\mathfrak{S} \subset W(R)$ ci-dessus s'étends en un morphisme injectif $\mathcal{O}_{\mathcal{E}} \to W(\mathrm{Fr}(R))$.
– Soit $\mathcal{E} \subset W(\mathrm{Fr}(R))[1/p]$ le corps des fractions de $\mathcal{O}_{\mathcal{E}}$ et $\mathcal{E}^{\mathrm{ur}}$ l'extension nonramifiée maximale de $\mathcal{E}$. Posons enfin $\mathfrak{S}^{\mathrm{ur}} := \mathcal{O}_{\mathcal{E}^{\mathrm{ur}}} \cap W(R) \subset W(\mathrm{Fr}(R))$, et $\widehat{\mathfrak{S}^{ur}} := \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \cap W(R) \subset W(\mathrm{Fr}(R))$.
– Enfin, l'inclusion $W[u] \subset W(R)$ ($u \mapsto [\underline{\pi}]$) s'étends en une inclusion $S \hookrightarrow A_{\mathrm{cris}}$, compatible aux Frobenius et aux filtrations.

Proposition 3.1. *Soit $\mathfrak{M} \in \mathbf{BT}^{\varphi}_{/\mathfrak{S}}$ et posons $\mathscr{M} := S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$. L'application canonique suivante*

$$\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{ur}}) \longrightarrow \mathrm{Hom}_{S,Fil,\varphi}(\mathscr{M}, A_{cris}), \quad f \mapsto \iota \circ (1 \otimes_{\varphi,\mathfrak{S}} f), \tag{1}$$

est un isomorphisme pour $p > 2$. De plus, les deux $\mathbb{Z}_p$-modules du morphisme (1) *sont libres de rang égal à* $\mathrm{rk}(\mathfrak{M})$*.*[5]

Dans la suite, $\mathfrak{M}$ désigne un objet de $\mathbf{BT}^{\varphi}_{/\mathfrak{S}}$ avec $\mathscr{M} := S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \in \mathbf{BT}^{\varphi}_{/,S}$.

Lemma 3.2. *Supposons $p > 2$. Le $\mathbb{Z}_p$-modules* $\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{ur}})$ *est libre de rang égal à* $\mathrm{rk}_{\mathfrak{S}}(\mathfrak{M})$*.*

Démonstration. Par les calculs de Fontaine (cf. les références dans Lemma 2.1.2 de [4]), le $\mathbb{Z}_p$-module $\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}/p^n\mathfrak{M}, \mathfrak{S}^{\mathrm{ur}}[1/p]/\mathfrak{S}^{\mathrm{ur}}) \cong \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}/p^n\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}}[1/p]/\widehat{\mathfrak{S}^{\mathrm{ur}}})$ est isomorphe à $(\mathbb{Z}/p^n\mathbb{Z})^{\mathrm{rk}(\mathfrak{M})}$. D'autre part, on a un isomorphisme canonique

$$\frac{\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}})}{p^n \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}})} \longrightarrow \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}/p^n\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}}[1/p]/\widehat{\mathfrak{S}^{\mathrm{ur}}}), \quad f \mapsto f/p^n.$$

Or, étant un sous-$\mathbb{Z}_p$-module fermé de $\widehat{\mathfrak{S}^{\mathrm{ur}}}^{\mathrm{rk}(\mathfrak{M})}$, le $\mathbb{Z}_p$-module $\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}})$ est complet pour la topologie p-adique. Par suite, en passant à la limite, on trouve $\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}}) \cong \mathbb{Z}_p^{\mathrm{rk}(\mathfrak{M})}$. D'où le résultat. □

Lemma 3.3. *Supposons $p > 2$. Soit $G \in \mathbf{BT}(\mathcal{O}_K)$. Il existe un isomorphisme naturel*

$$\mathrm{T}_p G \longrightarrow \mathrm{Hom}_{S,Fil,\varphi}(\underline{\mathscr{M}}(G), A_{cris}),$$

où $\mathrm{T}_p G$ désigne le module de Tate de G. En particulier, pour tout objet $\mathscr{M} \in \mathbf{BT}^{\varphi}_{/S}$, le $\mathbb{Z}_p$-module $\mathrm{Hom}_{S,Fil,\varphi}(\mathscr{M}, A_{\mathrm{cris}})$ *est libre de rang égal à* $\mathrm{rk}(\mathscr{M})$*.*[6]

Démonstration. Cf. l'exposé de Dajano. □

Démonstration de Proposition 3.1. Comme $\varphi\colon \widehat{\mathfrak{S}^{\mathrm{ur}}} \to A_{\mathrm{cris}}$ est injectif, et comme $\iota \circ (1 \otimes_{\varphi,\mathfrak{S}} f)$ est juste l'extension par scalaires du morphisme composé

$$\mathfrak{M} \xrightarrow{f} \mathfrak{S}^{\mathrm{ur}} \xrightarrow{\varphi} A_{\mathrm{cris}}$$

5. Dans [4], on trouve $\mathfrak{S}^{\mathrm{ur}}$ à la place de $\widehat{\mathfrak{S}^{\mathrm{ur}}}$ dans le morphisme (1) !

6. Il semble que dans les litératures, on montre d'abord le deuxième énoncé, puis en déduit le premier. Voir par exemple [3].

Par suite, le morphisme (1) est injectif. Or par les deux lemmes précédents, les deux $\mathbb{Z}_p$-modules du morphisme (1) sont libres de même rang, le morphisme (1) devient un un isomorphisme en inversant p. En particulier, pour finir la preuve, il suffit de montrer que, pour tout morphisme $f\colon \mathfrak{M} \to \mathfrak{S}^{\mathrm{ur}}$ tel que l'image du composé $\varphi \circ f$ soit contenue dans pA_{cris}, alors $f(\mathfrak{M}) \subset p\mathfrak{S}^{\mathrm{ur}}$. Pour démontrer ceci, on a besoin le fait suivant :[7]

Fait : le morphisme composé $\widehat{\mathfrak{S}^{\mathrm{ur}}} \xrightarrow{\varphi} A_{\mathrm{cris}} \to A_{\mathrm{cris}}/pA_{\mathrm{cris}}$ est de noyau $(E(u), p) \subset \widehat{\mathfrak{S}^{\mathrm{ur}}}$.

Pour finir la preuve, soit $f \in \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{ur}}})$ tel que $\mathrm{Im}(\varphi \circ f) \subset pA_{\mathrm{cris}}$. Par le fait ci-dessus, on a $\mathrm{Im}(f) \subset (E(u), p) \subset \widehat{\mathfrak{S}^{\mathrm{ur}}}$. Or $\mathfrak{M} \in \mathbf{BT}^{\varphi}_{/\mathfrak{S}}$, on sait $E(u) \cdot \mathfrak{M} \subset \mathrm{Im}(1 \otimes \varphi_{\mathfrak{M}})$. Par suite,

$$E(u) \cdot f(\mathfrak{M}) \subset \mathrm{Im}(1 \otimes (\varphi_{\widehat{\mathfrak{S}^{\mathrm{ur}}}} \circ f)) = \widehat{\mathfrak{S}^{\mathrm{ur}}} \cdot \left(\varphi_{\widehat{\mathfrak{S}}}\left((E(u), p) \cdot \widehat{\mathfrak{S}^{\mathrm{ur}}}\right)\right) \subset (E(u)^p, p)\widehat{\mathfrak{S}^{\mathrm{ur}}}.$$

Or $u^e = \overline{E(u)} \in \widehat{\mathfrak{S}^{\mathrm{ur}}}/p\widehat{\mathfrak{S}^{\mathrm{ur}}}$ est un élément régulier, on déduit que $f(\mathfrak{M}) \subset (E(u)^{p-1}, p)\widehat{\mathfrak{S}^{\mathrm{ur}}}$. Puis on continue et on a finalement $f(\mathfrak{M}) \subset p\widehat{\mathfrak{S}^{\mathrm{ur}}}$.

□

Références

[1] C. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*

[2] O. Brinon, *Théorie de Grothendieck-Messing, théorème de Serre-Tate Classification des groupes p-divisibles et représentations cristallines*, notes d'exposé.

[3] G. Faltings, *Integral crystalline cohomology over very ramified valuation ring*

[4] M. Kisin, *Crystalline representations and F-crystals.*

[5] B. Mazur, W. Messing, *Universal extensions and one dimensional crystalline cohomology*

[6] W. Messing, *The Crystals Associated to Barsotti-Tate Groups : with Applications to Abelian Schemes*

7. à vérifier